REMARKS

The Office examined claims 1-26, and rejected same. With this paper, claims 1-15 and 24-26 are canceled, and new claim 27 is added. Thus, claims 16-23 and 27 are now pending.

Request for Telephone Interview

To expedite prosecution in this application, filed now almost six years ago, applicant's attorney respectfully requests a telephone interview with the Examiner at the Examiner's earliest convenience. Applicant's attorney requests that the Examiner call applicant's attorney to schedule a telephone interview to review the invention as now claimed. Applicant's attorney would be assisted by another attorney, James A. Retter, Reg. No. 41266, who has permission from the owner of the subject patent application to participate in such a telephone interview.

Summary of claimed subject matter

As explained in the application at par. [0006], an object of the invention is detecting fraudulent use of a computer in engaging in online transaction. More specifically, the invention aims at providing a fraud detection mechanism that would ideally "only minimally affect [a] merchant's existing software and would route fraud detection efforts through a central, third-party entity serving a large multitude of merchants."

The invention uses a clever scheme to achieve its aim and thereby help detect use of a customer computer engaging in fraudulent transactions with one or more merchants over the Internet. The invention causes the browser used by the customer to embed a transaction identification string in a purchase request that results in a transaction (purchase of goods or services), along with what is called in the application a machine fingerprint, or machine data useable in creating a machine fingerprint (the machine being the customer computer hardware). The merchant then stores a transaction record (transaction string) indicating the details of the transaction, along with the transaction identification string. In addition, though, the invention causes the transaction identification string to be stored with the machine fingerprint, which is done in some embodiments at a third-party facility. Now, over time, the customer computer might be used to engage in transactions with the same and/ or other merchants who practice the invention so that for each transaction the merchant involved in the transaction stores a transaction identification string (provided by the third party in case of a three-party embodiment) with the *same* machine fingerprint, and (in case of the three-party embodiment), the third-party stores the transaction identification string for the transaction and again, the *same* fingerprint. So now one or more merchants have stored transaction identification strings with transaction records (the latter of which might well include confidential information), and the third-party has all the same transaction identification strings, each stored with the *same* fingerprint (and so the third-party does not know any confidential information). So if any transaction is believed fraudulent for any reason, the third-party can look up the machine fingerprint and determine all other transactions for the *same* fingerprint, and notify the one or more vendors they might have a problem. Notice too that the third-party does not have any of the actual transaction information, which could include personal or confidential information. Thus, one third-party facility can function as described for many different merchants and the merchants never have to worry that a customer's private information is outside their control.

As an illustrative example, transactions according to the invention as claimed can result in the following sets of records:

Merchant records		*Archive records*	
TX strings	**A. TX identifiers**	**TX identifiers**	**Fingerprints**
TX S1	TX ID1	TX ID1	Fingerprint-1
TX S2	TX ID2	TX ID2	Fingerprint-2
TX S3	TX ID3	TX ID3	Fingerprint-1
TX S4	TX ID4	TX ID4	Fingerprint-1

The merchant records may belong to one or more merchants, and stored at their respective facilities. The archive records may all be stored at one single facility, which may be the same or different than any of the facilities used to store the merchant records. As is evident now, the TX (transaction) IDs (identifiers) tie together the TX strings (that include the details of the transactions) and the fingerprints. So if e.g. the transaction with identifier TX ID4 is found out to be fraudulent, the invention allows the archive web site to be used to advise the merchants that transactions with identifiers TX ID3 and TX ID1 are possibly also fraudulent, since they were performed by the same computer (because they have the same fingerprint).

Changes to the claims

Claims 16-23 are changed and new claim 27 is added to more distinctly claim the invention in this respect. Support is provided at paragraphs [0036] and [0037] of the published application, i.e.:

> [0036] At step 46, the archive service 15 generates a unique transaction ID string and associates it with the customer machine parameter set in the MDAS archive 17. At step 48, the archive service returns the MDC script, with the transaction ID embedded within it, to the customer browser 28. At step 50, the customer browser 28 processes the MDC script which, at a minimum, writes the transaction ID string into the merchant's transaction form. Assuming that the customer 5 completes the transaction and submits the transaction form to the merchant 2 at step 52, the transaction ID string is stored with the transaction data record 6 in the merchant transaction database 7. The transaction ID, thus, indirectly associates the machine data parameter set 18 stored in the MDAS archive 17 at step 54 with the customer identity information stored with the transaction data record 6 in the merchant's transaction database 7. Thereafter, qualified parties may access the MDAS archive 17 for information related to a transaction ID.
>
> [0037] The MDAS archive 17 need not contain any information which specifically identifies a particular customer, only the machine parameter profiles 18 with associated transaction ID strings. The MDAS archive records 18 can be analyzed in conjunction with the merchant transaction records for patterns of fraud or for other purposes. The great majority of MDAS archive records can be purged from the archive 17 after a selected period of time. Any records which are associated with any transaction irregularities or suspicions of actual fraud may be retained longer.

With the invention, in case of three-party embodiment, if a merchant later discovers fraud in a transaction and alerts the third-party facility--called MDAS in the application--and identifies the fraudulent transaction by the transaction identification string (TX ID), MDAS can look up the machine fingerprint via the TX ID, and alert any other merchants who have transactions stored with the same machine fingerprint.

Here is another use of the invention, in case of either a two-party embodiment, where both the transactions and the fingerprints are stored in the MDAS and so are both accessible to a qualified party for analysis for patterns of fraud, or in case of a three-party embodiment where the qualified party has access to the transaction records of the various different merchants (see par. [0037], explaining that, "The MDAS archive records 18 can be analyzed in conjunction with the merchant transaction records for patterns of fraud or for other purposes."): For each transaction, a TX ID and fingerprint are stored, and the same TX ID and a transaction string (with customer identifying information and financial information, such as at least part of a credit card number) are stored. Then a qualified party can look to see if many different credit card numbers are associated with the same machine fingerprint, using the TX IDs to cross reference to transaction strings having the credit card information. In other words, the search is like this: Find a machine fingerprint record in MDAS. Get the TX ID for that fingerprint. Find the transaction for that TX ID, and examine the transaction string to obtain the credit card number (which may be a partial). Then find the next record having the same fingerprint, and get the TX ID for that record. Then find the transaction string also having that TX ID and get the credit card number for that transaction, and so on.

Rejections under 35 USC Section 102

In the final Office action, all the claims are rejected under 35 USC 102(e) as being anticipated by David (US 2002/0073046). David was filed after the instant application, but claims priority to an application filed earlier than the instant application, namely US Application Ser. No. 09/500,601, now abandoned, of which David is a Continuation-in-Part application, so that some of David might be new subject matter, first disclosed in David, after the filing of the instant application, and so of course would not be prior art. Applicant therefore understands the rejection to be based ultimately on the '601 application, and applicant further understands that the Office can and will rely only on subject matter disclosed in the '601 application (*and also* disclosed in David, per *In re Wertheim and Mishkin*, 209 USPQ 554, 564 (CCPA, 1981)).

The arguing here based on the '601 application, and not David, is consistent with the response made by the Office in the Final Office action to applicant's arguments that the portions of David cited in rejecting the claims (pars. 0075, 0076, 0133, 0139, and 0165) fail to suffice as prior art because of their lack of support in the application 09/500,601 of which David is a CIP. The Office responds the statement:

> The Examiner has reviewed the parent US application, 09/600,601, and finds support in its disclosure for the relied upon paragraphs of David used to reject the claimed limitations. ...

Thus, according to the Office, consistent with *In re Wertheim*, it is reference to the '601 application that is dispositive, not reference to David.

Applicant respectfully submits that the '601 application does not teach or suggest the invention as it is now more distinctly claimed. The '601 application is intended to provide a way for a consumer to safely make on online purchase, as opposed to guarding against fraudulent transactions (page 2, last full paragraph). In one embodiment (second paragraph, page 4) an ISP acts as a security service provider and simply verifies from time to time during a transaction that the "the subscriber is still signed in to the ISP computer system by verifying the identity of the computer currently actively communicating through the IP address." There is no teaching of how this is done, though. The '601 application explains in somewhat more detail (see Abstract) that what is disclosed there is:

> … a method for performing secure electronic transaction on a computer network, the network comprising a buyer's computer, a vendor server, a creditor server and a security server. The buyer's computer has a fingerprint file stored in the memory thereof. The method includes the steps of:
>
> i) the buyer computer requesting to purchase merchandise to the vendor server, the purchase request including said buyer computer's IP address;
>
> ii) the buyer computer selecting a predetermined form of secured payment method;
>
> iii) the payment method selection causing the vendor server to transmit to the security server a request for confirmation of the buyer computer's identify at the buyer computer's IP address;
>
> iv) the confirmation request causing the security server to send a retrieval request to the IP address, the retrieval request including a retrieval program for detecting and retrieving the buyer's computer's fingerprint file, and the retrieval request further comprising a response request asking for confirmation of the purchase request; whereby a positive response from the buyer's compute to the security server accompanied by the fingerprint file causes the security server to confirm the buyer computer's identity to the vendor server and to approve the purchase.

At no point in the '601 application is it ever disclosed on what basis the security server "confirms the buyer computer's identity." There is an implication that the fingerprint retrieved at the time of purchase is compared with an earlier retrieved fingerprint, but there is no teaching as to how this is done, i.e. there is no teaching of what is used to cross-reference the fingerprint obtained earlier and the fingerprint obtained at the time of the transaction. Applicant's attorney supposes it might be the IP address, but an IP address can change (so as to differ from one session to another), and so using the IP address does not make sense technically when the aim is to verify that the computer engaged in a transaction is the same as a computer engaging in an earlier transaction (if indeed that is an aim, and it is not clear that it is). At page 6, first paragraph of the Detailed Description, it is explained that:

> During the entire time the on-line session in progress [*sic*], the IP address does not change and is thus available as identifying information. By monitoring and occasionally re-verifying that the subscriber's computer is still on-line at the assigned IP address, the ISP can confirm that certain activities could be attributed to the subscriber.

This suggests that the IP address plays an important role, but there is no express teaching as to how the ISP "confirms the buyer computer's identity."

At page 8, third paragraph, the '601 application discloses an embodiment in which no fingerprint is used, but where the buyer's computer (BC) is determined to still be connected to an ISP via which a transaction with a merchant computer (MC) is being performed. In this, a request to confirm a buyer-code is evidently sent, from time to time during a transaction, to the IP address assigned by the ISP to the buyer's computer at log on. (This is therefore not in any way a teaching of the present invention, since no machine fingerprint is involved in any of the processing.)

At page 15, in the paragraph labeled "5," it is explained that a security service facility ("Creditor Toolbox") obtains from a customer computer "user information, UID and further identifying information about the user's computer ... for future reference." At page 14, it is explained that the security service facility "generates a fingerprint file including a unique identification ("UID") for the user using the identification characteristics of user's PC which ... accompanied the application." The UID thus apparently is what the '601 application calls the "fingerprint." (What use is made of the "further identifying information about the user's computer" referred to at page 15 is not explained.) At page 17, at the end of the first paragraph, at a point in a purchase according to the teaching of the '601 application where the customer is being asked to confirm before finally placing an order for the purchase, it is explained that:

> d) ... To accept the transaction, the user must provide his user password and submit the form back to the Toolbox [i.e. security service facility]. The form is accompanied transparently by the fingerprint file containing the UID and other machine identifying information decrypted and extracted from user's PC by the transmission from the Toolbox.

> e) If accepted by user, then Toolbox checks database to make sure user's credit limit is not exceeded and send s a coded confirmation to Merchant's server that the transaction confirmed ...

After all that is disclosed in respect to the UID/ fingerprint, there is not even an express teaching of it ever being used!

At any rate, there is no teaching or suggestion by the '601 application of any of the steps of the process of claim 16. Most importantly though, there is no teaching whatsoever of storing merchant records having a transaction string and a TX ID, and also storing archiver records, having a machine fingerprint and a TX ID, so that the TX ID can relate the two records, which makes possible all of the uses of the invention noted above.

Accordingly, applicant respectfully requests that the rejections under 35 USC §102 be reconsidered and withdrawn.

Conclusion

For all the foregoing reasons it is believed that all of the claims still pending in the application are now in condition for allowance and their passage to issue is earnestly solicited.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 4-25-07

By: John R. King
John R. King
Registration No. 34,362
Attorney of Record
Customer No. 20,995
(949) 760-0404

3691963
042507